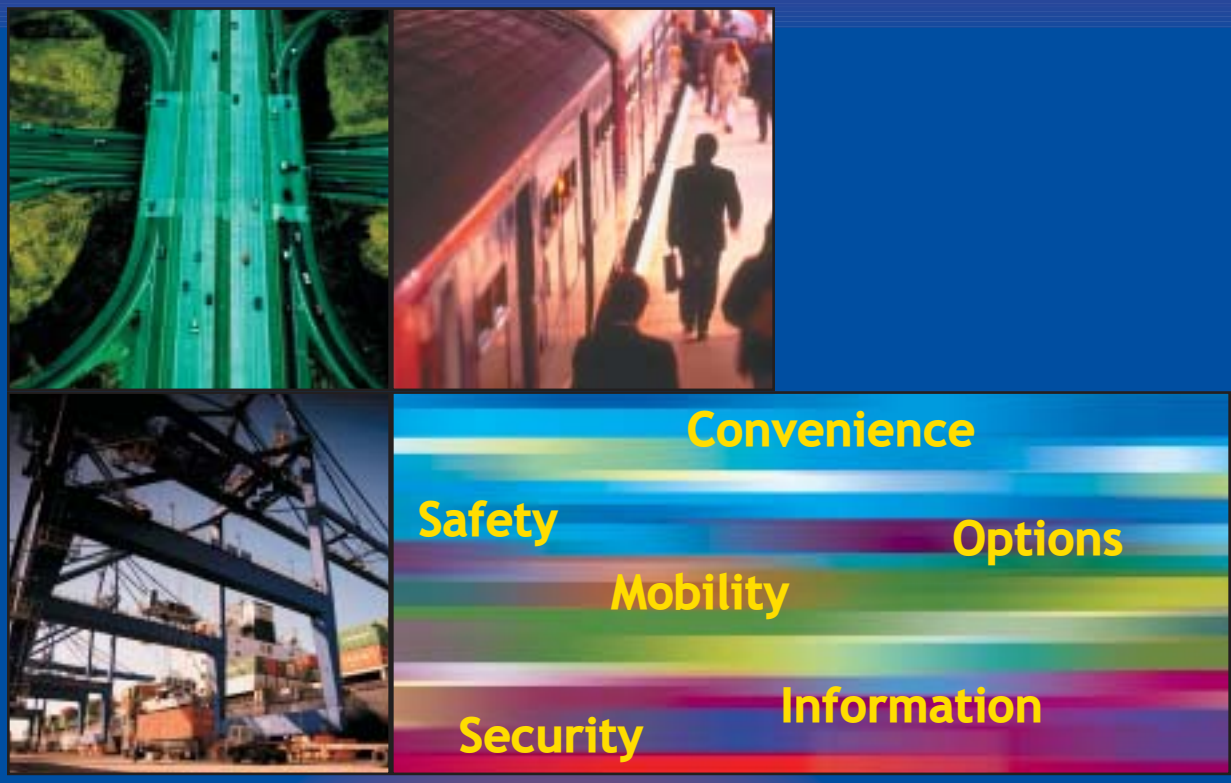
ITS America



Homeland Security and ITS

Using Intelligent Transportation Systems to Improve and Support Homeland Security

Supplement to the National ITS Program Plan: A Ten-Year Vision

September 2002

Prepared by the Intelligent Transportation Society of America in cooperation with the United States Department of Transportation

Homeland Security and ITS: Using Intelligent Transportation Systems to Improve and Support Homeland Security
Supplement to the National ITS Program Plan: A Ten-Year Vision

This material is based upon work supported by the Federal Highway Administration under Cooperative Agreement No. DTFH61-94-X-00076 and DTFH61-00-X-00006. Any opinions, findings and conclusions or recommendations expressed in this publication are those of the authors and do not necessarily reflect the view of the Federal Highway Administration.

Table of Contents

"Part of the challenge of homeland security is risk management. We can't protect ourselves 100% of the time against 100% of the risk against 100% of the possibility. But we can deploy our assets in a better way."

Gov. Tom Ridge
Office of Homeland Security

Introduction

"THE GOAL: A TRANSPORTATION SYSTEM THAT IS PREPARED FOR AND WELL-PROTECTED AGAINST ATTACKS, THAT RESPONDS RAPIDLY AND EFFECTIVELY TO NATURAL AND HUMAN-CAUSED THREATS AND DISASTERS, THAT SUPPORTS APPROPRIATE TRANSPORTATION, EMERGENCY MANAGEMENT, AND PUBLIC SAFETY AGENCIES, THAT ENSURES THE ABILITY TO MOVE PEOPLE AND GOODS EVEN IN TIMES OF CRISIS, AND THAT CAN BE QUICKLY AND EFFICIENTLY RESTORED TO FULL CAPABILITY."

>>The Intelligent Transportation Society of America (ITS America), in conjunction with the U.S. Department of Transportation, published the *National ITS Program Plan: A Ten-Year Vision* in January 2002. The Program Plan prescribed a broad set of policy, program, and research activities, enabled by ITS, to advance the safety, security, and efficiency of the surface transportation system. From an early stage, the design of the Program Plan included attention to technologies to detect, report, and respond to incidents ranging from traffic crashes to large-scale natural disasters. Several of the eight major themes in the Program Plan touch on these issues. For example, the theme "Automatic Crash and Incident Detection, Notification and Response" addresses tending the injured, evacuating those at risk, and returning the system to normal as rapidly as possible. In this theme, as elsewhere, ITS technologies are clearly applicable to human-caused disasters, whether deliberate or inadvertent, as well as to natural disasters and more routine incidents.

However, the events of September 11, 2001 raised the consciousness of the transportation community along with countless others, about the need for better critical infrastructure protection and crisis management, disaster planning and prevention, as well as effective detection and response, particularly in the case of deliberate terrorist attacks. The publication schedule for the Program Plan did not permit the development of a thorough treatment of this subject, although its importance was fully recognized. Starting from September 11th, ITS America and U.S. DOT assembled the resources to address the role of ITS in enabling and advancing the surface transportation aspects of Homeland Security. This supplement to the Program Plan is the result of that process.

One encouraging aspect of this analysis was the determination that large parts of ITS, already in progress to meet safety, mobility, and efficiency goals, are directly

applicable to enhancing Homeland Security. This is true both for ensuring the security of the transportation system and for supporting the efforts of other stakeholders, most notably planners and first responders. While additional attention is now being given to expanding ITS capabilities specifically for Homeland Security purposes, many existing ITS capabilities are already being deployed to further this purpose.

This supplement follows the same general structure as the Program Plan and draws some of its content from materials in the published version of the Program Plan. It includes:

- The restatement of the Ten Year Vision and an updated Security Goal for ITS.
- A new major theme: *Homeland Security*, incorporating:
  - Current status and opportunities.
  - Benefits.
  - Challenges.
  - Needed research, program, and institutional actions.
- Stakeholder roles in achieving the Ten Year Vision in the area of Homeland Security.

Vision and Goals

>>This section reiterates the ITS Vision and updates the Security Goal from the Program Plan to provide context and continuity. The ITS Vision is to ensure that:

- Future transportation systems will be managed and operated to provide seamless, end-to-end intermodal passenger travel regardless of traveler age, disability, or location; and efficient, seamless, end-to-end intermodal freight movement.
- Public policy and private sector decision makers will seize the opportunity to make ITS a vital driver in achieving the vision of the transportation system for the 21st century.
- Future transportation systems will be secure, customer-oriented, performance-driven, responsive in times of crisis, and institutionally innovative, enabled by information from a fully integrated spectrum of computing, communications, and sensor technologies.

Joining goals for safety, efficiency/economy, mobility/access, and energy/environment, the Program Plan includes a Security Goal.

Security

Unlike some natural disasters that can be anticipated, terrorist attacks are sudden and unexpected. Even if we have some information on a possible attack, we will generally not know exactly where, when, or how an attack will occur. Without this information, the most effective strategy is to plan in advance, to prevent and mitigate where possible, and to respond when necessary with flexibility, coordination, and speed. The transportation system and ITS will play a major role in the restoration of services and of the economic vitality of the affected area.

The ITS community agrees that

> *"This type of strategy requires management coordination, compatible communication systems, and real-time information feedback to decision-makers that permits near immediate changes in strategy when required. This approach also requires mechanisms for disseminating information to the general public that provides the most up-to-date guidance on the best transportation options for avoiding bottlenecks in the transportation system."*[1]

ITS provides tools and enhanced opportunities to help safeguard the transportation system against a variety of threats, both natural and human-caused, help the transportation system and its operators react swiftly and responsively in case of disruptions, and materially help agencies with primary responsibility to respond, by:

- Providing surveillance and analysis for freight and intermodal operations: monitoring and maintaining the security of containers on trucks and trains and in cargo handling facilities, monitoring other mobile assets, matching cargo against bills of lading, matching actual travel against intended routes and destinations, and assuring the identity of commercial operators.
- Providing surveillance and analysis for public transportation, including identification of and effective rapid response to threatening or high risk passenger behavior, matching actual travel against planned routes and schedules, assuring the identity of transit vehicle operators, and providing surveillance and analysis at major transportation centers.
- Providing surveillance of other major transportation facilities, including bridges and tunnels, and operations, management, and response centers.
- Safeguarding ITS systems and data (as well as other transportation-related computer controlled systems) against inadvertent or deliberate interference, destruction, and misuse.

[1]FOOTNOTE needed here

- Providing logistical and communications tools to:
  - Enhance existing and emerging capabilities of transportation, law enforcement, defense, emergency response, and security organizations to plan and execute swift, appropriate, and coordinated responses to system disruptions.
  - Help rescue and treat the injured.
  - Clear roads and rails, smoothly reroute travel to available alternatives, and restore services as promptly as possible.
  - Provide the public with prompt and accurate information on transportation alternatives in case of disruptions to portions of the system or when quarantine or evacuation is necessary.
- Helping to assure that vehicle and drivers licenses, particularly commercial licenses, are issued and used appropriately.

The goal is a transportation system that is prepared for and well-protected against attacks, that responds rapidly and effectively to natural and human-caused threats and disasters, that supports appropriate transportation, emergency management, and public safety agencies, that ensures the ability to move people and goods even in times of crisis, and that can be quickly and efficiently restored to full capability.

What ITS Can Do

>>This Security Supplement focuses on five broad areas for the application of ITS to Homeland Security: Preparedness, Prevention, Protection, Response, and Recovery. The remainder of this Supplement expands on the theme of ITS and Homeland Security in terms of these five areas. The following summarizes the capabilities and contributions that ITS provides in each area.

ITS Capabilities for Advancing Homeland Security

Preparedness

- Data and tools for analyzing the transportation system, identifying vulnerabilities and to plan in advance for contingencies by conducting "what-if" analyses under various scenarios.
- Tools and technology to facilitate communication and coordination among transportation agencies and between transportation agencies and other stakeholders including response agencies and the general public.
- Basis and framework for training and testing for emergency situations.

Prevention

- Sensors and analysis capabilities to detect and head off threats along roads and rails, at transportation centers (depots and operations/management centers), and for other portions of the infrastructure (bridges, tunnels).
- Capabilities to guard against misuse of commercial vehicles and halt deviating vehicles.
- Analogous capabilities for transit and rail, including continuous surveillance of the road/rail infrastructure against tampering or misuse.

Protection

- Tools and technology for on-site detection and response to potential threats to facilities and systems.
- Tools and technology for hardening and coordinating transportation-related communications and information systems.
- Tools and technology for establishing and activating alternate routes in times of emergency for vital personnel and materials, and escape/evacuation routes.
- Tools and technology to increase the ability of other agencies to undertake protection activities.

Response

- An architectural framework and technologies to maintain communications and facilitate coordination among responding agencies.
- Tools and technology for determining and disseminating accurate, up-to-date information about the state of the transportation system both to responders and to the general public.
- The ability to provide information about the status and location of vehicles carrying hazardous materials in the vicinity of a crisis scene.
- Tools and technology for rerouting traffic when the system is impaired or under attack.

Recovery

- Tools and technology to create a flexible, reconfigurable transportation system to meet emergency needs.
- Enhanced ability to execute plans for alternative modes/alternative routes in emergency situations.
- Tools and technology to make maximum use of available capacity through load balancing.

What the ITS Industry Should Do

>>This Security Supplement contains a wide range of recommended research, program, and institutional actions and makes a large number of suggestions regarding recommended roles for various stakeholders in and around ITS. All of these recommendations are important. However, a few overarching recommendations for action deserve special mention:

Develop a national, transportation-specific security doctrine that focuses on all transportation modes. The national security community and transportation community – public and private – are focusing their limited resources on priority issues. There has been little opportunity to develop a comprehensive array of policies and procedures for all modes. Over time, the complete range of threats, vulnerabilities, and countermeasures needs to be considered

Accelerate the deployment of ITS-based transportation security technologies. Many ITS technologies are already available to enhance Homeland Security. Wider and swifter deployment of these technologies will support Homeland Security in general, and will also help to protect the transportation system on which so many Homeland Security stakeholders depend.

Create an Integrated Network of Transportation Information. This recommendation from the base National ITS Program Plan becomes all the more urgent in an environment where security concerns are heightened. The INTI will be a fundamental tool for managing the transportation system and disseminating information to its users both for normal operations and in times of crisis.

Encourage the Use of Telematics and Intelligent Vehicle Technology. Smarter vehicles and better communications are a fundamental key to better surveillance and to controlling events and disseminating vital information in times of crisis.

Support Security-Enhancing Commercial Vehicle Technology. Commercial vehicles are a major and ubiquitous component of the economy. At the same time, commercial vehicles represent a resource that can be misused for terrorist activities. Better technology is needed to recognize and track potentially hazardous cargo, to assure that a commercial vehicle is being driven by an authorized person along an appropriate route, and to safely halt commercial vehicles which deviate from these guidelines.

Expand Security-Related ITS Research & Development. Much valuable ITS technology to enhance security is already available. More and better technology is needed to allow ITS realize its full potential to enhance Homeland Security.

Support Regional Cooperation to Enhance Security. In the current environment, public sector action must be regional, not just local. Recent experience with both natural and human-caused disasters underscores the need for cooperation, communication, and joint planning among the agencies both within a jurisdiction and across jurisdictions.

Support Public-Private Cooperation. Both in general and in the worlds of transportation and ITS, successful approaches to security require participation both from government and industry. This is an ideal time to forge new relationships and partnerships to assure the best possible planning, protection, and response.

"Smart transportation can teach the rest of us how to do smart security, how to move goods, information and services in a way that is both secure and efficient."

Sandy Berger
National Security Advisor
to President Clinton
ITS America's 2002 Annual Meeting
and Exposition, April, 2002

Homeland Security

Current Status + Opportunities

>>The terrorist attacks of September 11th made many things clear. First, despite devastating attacks, the surface transportation system taken as a national whole was not seriously disrupted. Second, the characteristics of the transportation system that we strive for—to be open, accessible, free-flowing and convenient—can leave us vulnerable to deliberate disruptions. Third, and possibly most important, the transportation system and existing ITS capabilities had multiple roles in the response to and the recovery from the terrorist acts, many of which roles were in support of other agencies involved in public safety and relief efforts. Finally, ITS has wide applicability in future efforts to anticipate, deter, and respond to terrorist acts and other disasters.

A preliminary post-September 11 analysis in New York undertaken by the U.S. Dept. of Transportation found that New York City's adoption of an Incident Command System was of great service in responding to the attacks. Staff had been trained to respond to emergencies both within and across agencies. Pre-existing relationships among key personnel enabled the institutional coordination that was key to successful emergency management. Data, including transportation system data, collected and manipulated by advanced technologies, aided decision-making. Redundancy built into institutional and physical systems was an important factor in responding to the emergency and restoring the system. One problem was the disruption and overloading of public wireline and wireless communications systems. Consideration is now being given to reserving portions of wireless capacity for security needs to minimize this problem in the future.

U.S. DOT found this situation to be similar in many respects to the one surrounding the 1994 Northridge Earthquake near Los Angeles. The adoption of an Incident Command System by that region provided it with a pre-existing structure for coordinating decisions among multiple state, local, and Federal agencies. These procedures allowed the region to respond better and more quickly. The use of innovative bidding and construction methods helped expedite the reconstruction process and restore freeway mobility to the region. Existing state and local traffic management centers, which were in operation before the earthquake, helped manage the resulting traffic diversions.

The lesson is clear. Advance planning and the establishment of smooth working relationships among multiple public agencies and other stakeholders are crucial in dealing with extraordinary situations. These same steps have widespread benefits for routine operations as well.

The transportation system will continue to have multiple roles in responding to disasters, both natural and human-caused. Its ability to fulfill these roles depends on a continuing improvement in its capabilities and in the relationships among stakeholders. Terrorist attacks cannot all be stopped. However, the tools provided by ITS, both those already available and those under development, will be major contributors to this improvement. ITS will help move goods and people and help support the efforts of both transportation and non-transportation agencies, in both routine and exceptional circumstances. ITS offers great promise for helping to prevent attacks as well as for responding to the full range of incidents, large and small, regardless of origin.

One major need is to better educate the owners and operators of traditional transportation infrastructure on the capabilities and additional leverage that ITS provides for more effective planning, for better and

more efficient routine system management, and for speedy response and inter-agency coordination in times of crisis.

Technologies in use today in surface transportation can be adapted to make the infrastructure and the traveler more secure. Some of these technologies include smart cards, biometrics identifiers, automatic vehicle location, map databases, video, motion, and infrared detection and surveillance, vehicle classification sensors, weigh-in-motion technology, and geolocation and routing technologies to track the movement and behavior of vehicles, particularly commercial and transit vehicles. Technologies exist to identify vehicle contents, particularly hazardous substances, explosives, and drugs, without opening the vehicle. Technology is available to match a specific commercial vehicle with a specific operator and a specific cargo and to notify authorities and prevent or halt travel in case of a mismatch. Simply doing better surveillance has deterrence value.

Furthermore, if an attack does occur, many of the sensor, communication, and analysis technologies used today to better manage travel and transportation can be adapted to assess damage and facilitate recovery, evacuation, and quarantine. Current technologies include vehicle probe data, advanced signal systems, signal priority and preemption systems, moveable lane barriers, dynamic message signs, incident detection systems, mayday systems, and public safety response systems. Traffic management centers, fleet dispatch centers, and telematics services perform portions of this function today. Communications devices available to truck and transit drivers and operators may also be employed to report suspicious activity.

At the same time, the ITS industry must diligently continue to expand and refine ITS capabilities, interact constructively with other fields (e.g., aerial surveillance), and continue to provide new tools for building relationships among stakeholders and providing them with the tools they need to operate effectively.

The tools and technologies of ITS have made and will continue to make major contributions to Homeland Security. ITS capabilities are essential to Homeland Security in general, both directly and in support of non-transportation agencies that have the primary responsibility to prepare for, detect, prevent, and respond to threats, whether natural or human-caused. Direct contributions to general Homeland Security focus on preventing the transportation system—infrastructure, facilities, and vehicles—from being used to carry out attacks against any homeland target. In addition, ITS is a key tool for safeguarding the security of the transportation system itself against threats. This includes physical threats and threats against related information and communications systems. It also includes working to prevent cascading failures both within the surface transportation system and across other adjoining systems.

There are five broad areas where the transportation system and ITS have a significant role in advancing Homeland Security:

- Preparedness
- Prevention
- Protection
- Response
- Recovery

While each of these areas has its own characteristics, there is not always a hard line of demarcation between them. For example, preparedness interacts with them all. The sections which follow define each of these areas and outline the role of transportation and ITS in meeting the needs of each area, both directly and in support of others' efforts.

PREPAREDNESS

Preparedness starts with understanding the scope and magnitude of the security problem: What are the threats and the resultant vulnerabilities? Where can existing technology be applied to reduce vulnerability? What are the gaps that need to be closed? How can appropriate information be better delivered to the public and shared completely and securely among cooperating agencies? The conduct of vulnerability analysis will provide the focus for setting priorities in this stage. A continuing assessment of vulnerabilities will lead to identification of shortfalls in system preparedness which then leads to the appropriate investment in countermeasures.

More than anything else, preparedness requires coordination. It requires engaging relevant stakeholders from the transportation industry and interacting with relevant stakeholders in multiple other industries. Joint operational procedures, message sets, and mapping concerns are among the areas to be addressed in this stage.

Vulnerability does not relate only to potential disruption of the transportation system. It also relates to the implications of this disruption: the ability to move personnel and equipment, food and medicine, and to evacuate people at risk.

Preparedness means developing a range of emergency scenarios and making (and periodically testing) plans to respond to each scenario. For example, ITS map databases and analysis techniques can help identify single-threaded or constricted points of flow whose disruption could complicate both escape from an affected area and access by emergency services. Once identified, these bottlenecks can be eliminated by establishing alternative or expanded paths of flow. More and better data is essential on the location of assets (e.g., fire hydrants for easier location; exits and entrances of buildings and strategic facilities) and the connectivity of road networks. Information must be shareable across jurisdictions.

Preparedness includes conducting training and exercises to increase the system's overall response capability and to evaluate the validity of plans and their underlying assumptions.

PREVENTION

Prevention means taking steps to counteract potential threats before they occur. This includes creating an environment that deters potential attackers from making an attack and thwarting attempted attacks before they can be carried out or completed.

Traditionally, deterrence includes creating a high level of certainty of capture and punishment for hostile acts. This approach should clearly not be neglected. However, it will not be effective for terrorists who are willing, or worse, eager to die during their attacks. Therefore deterrence must also be aimed at lowering the probability that an attack will be successful or effective.

One concern is the unregulated and unsupervised movement of vehicles containing potentially hazardous materials. The attacks of September 11th were carried out using commercial aircraft. However, as the Oklahoma City bombing demonstrated, it is also possible to cause great damage and loss of life using surface vehicles carrying explosives. Experience in the Middle East and Northern Ireland shows that even small-scale terrorist attacks involving cars and buses can be extremely disruptive. These kinds of threats all need better deterrence. Geofencing and the profiling of certain types of for-hire vehicles are being discussed.

In general, prevention requires careful advance planning to understand threats and the mechanisms that can be used to prevent them. It then requires the deployment of these preventive mechanisms. Such mechanisms will often include greater information gathering and sharing, surveillance, and diligent coordination and cooperation among multiple stakeholders.

Within surface transportation, prevention clearly includes better security at points of entry to the U.S., better intelligence on threats, and better identification and tracking of potentially hazardous materials.

To provide the highest level of prevention it is critical that all aspects of the surface transportation network—road, rail, air, and sea—be interconnected to enable the comprehensive analysis that will identify potential threats. The knowledge that this analysis occurs can provide deterrence.

Global positioning device on a truck provides security for driver, vehicle and cargo.

PROTECTION

Protecting the transportation system itself is a primary responsibility of the transportation and ITS communities.

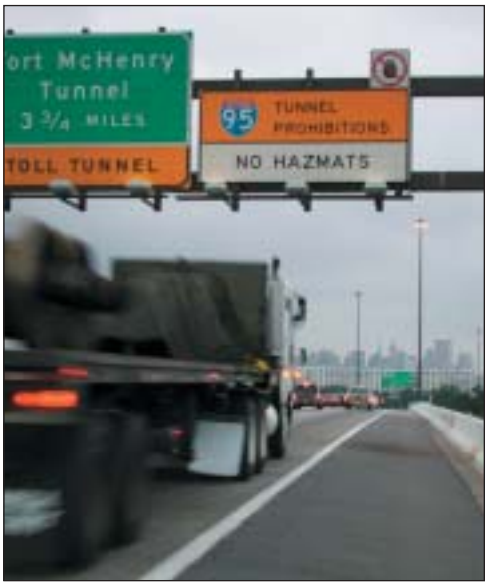
Protection means warding off attacks and minimizing their consequences. This is done by making attack targets less vulnerable and by recognizing and thwarting attacks that are in progress. Many of the mechanisms already in place for dealing with incidents and natural disasters will also be essential for protecting against attacks.

Within surface transportation, the focus is on ensuring the network's ability to support responses to attacks and natural disasters and to rapidly restore services. The first avenue of protection is to identify and harden vulnerable portions of the transportation system against attack, including both physical facilities and information/communications systems. Physical facilities include the infrastructure itself (roads, rails, waterways, ports, and associated equipment) and related operations and control centers. Military experience and technology from earthquake proofing provide some background, but this practice is still in an early stage of development and significant research is necessary.

Minimizing the consequences of attacks also means providing for alternate transportation routes and system redundancy at strategic points. This will help to assure that vital materials and service personnel can be moved where they are needed and that evacuation and escape can be better assured.

Protection also means detecting the fact that an attack is being planned or being mounted. ITS, along with the other information technologies, provides important tools for pattern recognition and analysis, looking for the suspicious or questionable circumstances: patterns which are either unusual or which fit predetermined templates for terrorist behavior. All modes of the surface transportation system, including road vehicles, transit vehicles, and trains, can make additional contributions to detection, given appropriate planning and equipment. This capability can be enhanced via cooperation with other facilities, like aerial and satellite surveillance.

One key area of protection for which ITS technology is central is the ability to safely halt surface vehicles that have been identified as threatening. One example is commercial vehicles containing hazardous materials that have gone off route, particularly in the vicinity of critical facilities. This and other aspects of protection imply the need to be able to appropriately interpret telemetry and intelligence and to get the information to the right place for action.

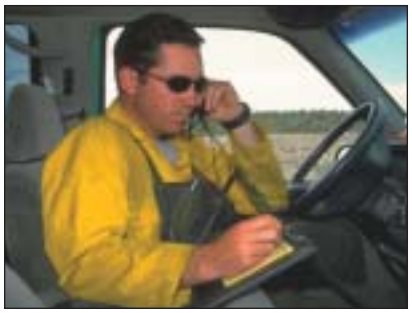


RESPONSE

Response begins with the recognition that an attack or a natural disaster is underway or has occurred. A particularly important role of ITS in this stage is to support responding agencies and help them to be more effective. Response will be most effective when advance planning has been done, covering as many contingencies as possible. More than anything else, response should mean *executing* the plans that were previously developed in anticipation of a crisis. One critical item of advance planning is establishing mechanisms for communications and coordination among responders. This is notably an area in which preparation for crisis situations will have significant beneficial effects on routine operations as well.

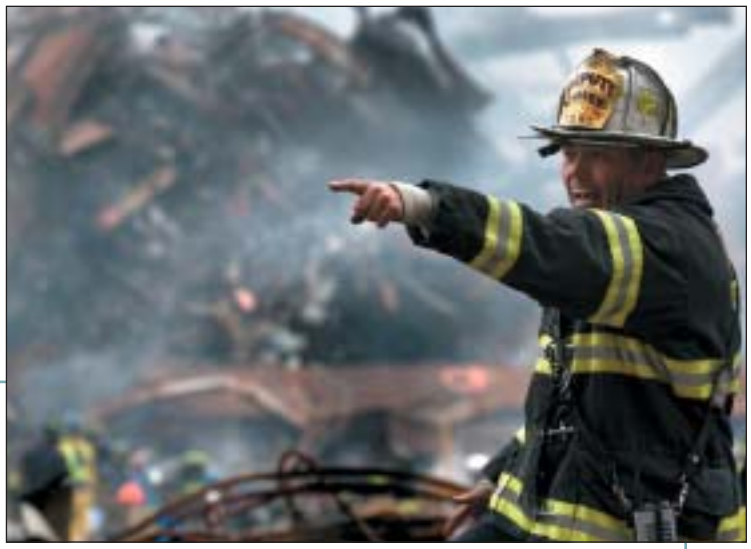
The transportation system has the responsibility to help provide information on incidents to responders and to the general public. It also has the responsibility to get responders to the site and get the public both out of danger and out of the way of responders. First responders need to know the status of the road network—traffic, weather, strength of bridges, overpass height—and the quickest real-time route to response sites. Evacuation and emergency access needs may have to be met simultaneously. System status and traffic management technology is essential to both these functions.

If the transportation system itself has come under attack, a primary concern is to keep the system running or get it back in operation, at least at a minimum level. This is an area in which the sensor, computing, and communications technologies that define ITS will be of particular importance. The identification and management of hazardous materials in a disaster area, especially those that were in routine transit when the crisis occurred, will depend heavily on ITS.



RECOVERY

Recovery means bringing the system back to normal, or as close to normal as possible, following an incident. If an incident is a major crisis, whether natural or human-caused, recovery will generally occur in a series of stages. Early stages of recovery may include providing basic services to a limited service population, with gradual moves toward normal service for everyone. Recovery may include deploying alternatives to regular service: buses rather than trains, different from normal driving routes, the use of priority corridors to move critical goods and services to/from a response site, etc. In all stages of recovery, providing good information to the public on current status and next steps is vital. ITS will be crucial in generating, evaluating, and implementing alternatives, tracking and supporting the return to normal service, and disseminating information across agencies and to the public.



Retired fire chief Joseph Curry barks orders to rescue teams as they clear through debris that was once the World Trade Center Sept. 14, 2001, in New York.

SYSTEM AND DATA SECURITY

At its most basic, ITS helps communicate information about the transportation system to support its operators and users. As previously observed, attacks and natural disasters can result in the disruption and destruction of these information and communications systems as well as the physical infrastructure. In addition, information and communications systems are potentially vulnerable to hacking, deliberate overloading, denial of service, and other technology-driven interference as well as to physical attack. The potential for this kind of interference increases as transportation systems come to depend more on information, software, and communications. This growing dependence on ITS technologies to operate a modern transportation system creates a critical need for:

- Protecting the availability, integrity, and confidentiality of data.
- Reducing the vulnerability of systems and services and ensuring the continuity of operations.
- Guarding against the effects of cascading and escalating failures in multiple interconnected systems, both within the transportation industry and across multiple industries.

Data Concerns are not new and are obviously not restricted to transportation or ITS. However, these concerns become central as the ITS industry proceeds with the development of the Integrated Network of Transportation Information prescribed in the *National ITS Program Plan*. The Integrated Network will interconnect and help to coordinate large numbers of information systems across many jurisdictions and geographical areas. Consistency and integrity are crucial to its effective operation. At the same time, integration potentially increases the risk of single point failures with widespread consequences, and information coordination needs strong safeguards to assure the maintenance of privacy.

System Vulnerability has the potential of increasing as systems become more widespread and comprehensive. As systems grow more critical, they become increasingly attractive targets for malicious interference. Increased insistence is needed on rigorous system engineering and security design processes to help ensure the integrity and impregnability of these systems.

Cascading Failures can occur when systems are interconnected and mutually dependent on one another. The classic historical example of a cascading failure is the 1977 electrical blackout on the East Coast, in which a failure in one power grid caused overloads and consequent failures in adjoining grids across a wide area. Interconnecting systems must be mutually supportive, especially in crisis situations. However, they must not become so dependent on or intertwined with one another that a single point failure can cause the entire network to collapse. Both planning and comprehensive testing across a wide range of possible scenarios is key to avoiding cascading failures.

Homeland Security

Benefits

A MORE SECURE TRANSPORTATION SYSTEM

>>ITS has contributions to make in all of Preparedness, Prevention, Protection, Response, and Recovery.

- ITS facilitates **Preparedness** by providing data and tools for analyzing the existing transportation system, identifying potential vulnerabilities, and conducting wide-ranging "what-if" analyses to understand the consequences, both positive and negative, of various approaches to transportation-related Homeland Security. Possibly most important, ITS provides tools and technologies to enable and enhance communication and coordination among multiple stakeholders, notably including transportation and public safety agencies. It also provides the basis and framework for the development of comprehensive training and exercise programs at all levels.
- ITS facilitates **Prevention** through the use of sensors and analysis capabilities that can detect and head off threats in the making. For example, ITS provides capabilities to verify that commercial vehicles carrying hazardous materials are being driven by the right person along the right route, to safely and automatically halt vehicles which fail this verification, and to swiftly notify authorities of such situations.
- ITS facilitates **Protection** by providing on-site detection and response to potential threats to facilities and systems and by helping to harden and coordinate transportation-related information and communications systems. ITS also provides the tools for establishing and activating alternate routes to keep vital materials and people moving and to facilitate evacuation and escape. ITS capabilities increase the ability of other agencies to protect critical elements of the overall infrastructure.
- ITS facilitates **Response** by providing an architectural framework and technologies to maintain communications and facilitate coordination among responding agencies. ITS facilitates the mobility of responding agencies through its ability to modify and adapt traffic flows. ITS also provides the basis for determining and disseminating up-to-date information about the state of the transportation system, both to assist responders and to inform the general public. This information notably includes the status and location of vehicles which were routinely carrying hazardous materials in the vicinity of a crisis scene.
- ITS facilitates **Recovery** by helping to create a flexible, responsive transportation system, which can be managed and reconfigured to meet emergency requirements, including the delivery of information to the public on what to do and what to avoid. ITS also provides the means to maximize the utilization of available capacity through load balancing the transportation network.

A MORE SECURE TRANSPORTATION SYSTEM, continued

The damage from terrorism goes beyond the physical destruction and personal injury from the immediate attack. Damage also results from a loss of confidence in the system and a heightened sense of risk associated with the everyday activities of living. ITS can help minimize and counteract these effects by providing the ability to accurately assess and report on the state of the transportation system both to public agencies and the public, and by providing a higher level of confidence that further attacks will be detected and thwarted. Such confidence may also have a deterrent effect.

Altogether, ITS can help provide a transportation system that is more secure, better able to respond to crises of any kind, and well-equipped to aid and support the many agencies, both within and outside the transportation arena, involved in all aspects of security.

BETTER SECURITY CAN PRODUCE BETTER EFFICIENCY

The concern is often expressed that heightened security measures bring complications, delays, inefficiencies, and additional costs to life in general and to transportation in particular. However, with careful planning, many important aspects of heightening security can actually promote efficiency and economy. It is worth noting that the original motivation for the Interstate Highway System was to facilitate the movement of defense personnel and materiel. However, the beneficial effect of the system on American life in general has been profound.

Responding to security concerns by increasing the level of communications and coordination among public agencies (including transportation and public safety agencies) and between these agencies and other stakeholders (including travelers and shippers), will help to promote a more smoothly functioning transportation system across the nation.

For example, heightened concerns about the conveyance of hazardous materials can help lead to a more seamless and efficient freight management environment. Such an environment can provide better, quicker, and more reliable information to shippers, carriers, and relevant agencies, lowering costs and increasing efficiency throughout the supply chain. Similarly, crisis planning for transportation can lead to better and more robust intermodal facilities and better and more accessible transportation alternatives both for people and goods. These will be essential in times of crisis, but will also provide better, less expensive, more flexible service for routine travel during the vast majority of time when no crisis is present.

"INTEGRATED NETWORK of TRANSPORTATION INFORMATION" HELPS OPERATIONS and SECURITY

The events of September 11th make it clear that the Integrated Network of Transportation Information, already envisioned in the January 2002 *National ITS Program Plan,* is more than a comprehensive information tool for better infrastructure management and traveler services. It is also the foundation for ensuring a safe and secure transportation system and for enhancing the security of all the services in the U.S. economy that depend on transportation. In addition to supporting transportation directly, ITS and its major programs will provide direct support for the missions of non-transportation agencies. Increased efficiency, economy, and responsiveness in many areas will benefit from streamlining, information exchange, and cooperation in the transportation sector through the tools of ITS.

programmatic theme 5

Homeland Security

Challenges

Many of the challenges described here apply both to transportation/ITS and to other interests and industries.

- **Security vs. Privacy** When formerly unconnected information systems are integrated and coordinated, the right to privacy is potentially more readily compromised. Heightened security concerns may have the potential of impacting other Constitutional rights as well. Determining the right tradeoff and implementing mechanisms to safeguard these rights without risking security will be an important and ongoing challenge.
- **Security vs. Mobility/Cost/Efficiency** It was observed above that the skillful implementation of security measures can actually improve the performance of a complex, multi-faceted system. However, achieving these goals simultaneously will not occur without extremely careful analysis, planning, and execution. Without such care, there is a significant risk that security measures could obstruct mobility and adversely affect costs and efficiency.
- **Technology** Many ITS technologies that are already well understood and available can promote the security of the transportation system and support the security efforts of both

transportation and non-transportation stakeholders. However, improved sensors and other hardware technology, improved wired and wireless communications networks, and new, better software and analysis tools are needed, particularly to support the prevention and detection of threats.

- **Technical Complexity** Smoothly integrating security features into already complex transportation systems will require careful planning and execution. Particular care must be taken to address data security and system vulnerability concerns, which can be exacerbated as systems become larger and more interconnected.
- **Multiple Layers of Security** A particularly important consideration is that the technology used to enhance security must itself be highly secure. To illustrate, the first-approximation technologies for bringing errant commercial vehicles to a halt, that were described at the 2002 ITS America Annual Meeting, are presently far too vulnerable to improper activation by unauthorized people. Misuse of such technology could create a crisis of its own. The electronic and communications systems and the processes used to protect against and respond to attacks and natural disasters must themselves be well guarded against attack, tampering, and hacking.
- **Funding** Getting access to funding to advance security interests may be difficult, despite the increased available of such funding from Federal and other sources. The highly distributed nature of surface transportation and ITS, both geographically and administratively, presents special challenges in securing and coordinating funding. Making a coherent funding case for ITS—a multidisciplinary, public-private undertaking—will be a challenge. In addition, the funding of ongoing operations and maintenance of ITS-enabled security measures is an issue separate from development, but one that is equally complex and demanding.
- **Institutional Challenge** Requirements for and execution of ITS-enabled security measures are intrinsically local; development and funding are intrinsically national; coordination is an issue at all levels. Creating ITS solutions that are responsive to local needs and getting them built, installed, and effectively operated and coordinated will be a significant organizational challenge.
- **Community Involvement** Public transit safety and security in particular depend on an involved community that helps watch for problems and whose own requirements for safety and security are well understood by service providers. Mechanisms for such involvement are not widely in place.

Workers guard the entrance to the crash site at the Pentagon on Sept. 14th. Damage to the Pentagon was caused by a hijacked commercial jetliner crashed into the Pentagon on Sept. 11.

Homeland Secirity

Actions

RESEARCH

- Explore and identify appropriate techniques and technologies for threat assessment, including identifying the types of threats to be assessed and the vulnerability of transportation facilities and ITS resources.
- Develop technology to improve automated detection and surveillance of vulnerable facilities as a key protective and deterrent measure. Private sector entities have a range of available products and infrastructure which should be reviewed for applicability.
- Explore techniques and technologies for determining (and as necessary creating in advance) alternate transportation paths for use when portions of the system are out of service. Alternates may include mode shifts as well as route changes. Make sure the needs of mobility impaired people are included. Particularly explore methods for identifying and relieving points of constricted flow to keep areas from being isolated due to attacks or natural disasters at these points and to avoid bottlenecks when evacuation is necessary.
- Explore methods for developing and maintaining base maps that facilitate interconnection with emergency management, defense, and public safety agencies. Determine methods for identifying and resolving other interconnection issues (frequencies, clock time, data security) that currently hinder coordination among these agencies.
- Determine needed types and placements of sensors, in the infrastructure and in vehicles of all kinds, to identify potential threats and detect disruptions to normal operations. Develop analysis tools to fuse sensor data into meaningful information that can be swiftly acted upon.
- Develop and test new and better methods for sensing and identifying hazardous materials.
- Develop algorithms for managing traffic signals and other traffic control devices specifically tailored to crisis response and evacuation.
- Participate, across modes and industries, in network analysis research related to avoiding and preventing cascading failures.
- Develop systems for commercial vehicle tracking to assure that commercial vehicles are carrying the right cargo along the right route under control of the right operator.
- Develop systems for public transit tracking to monitor passenger behavior and to assure that public transit vehicles are traveling along the right route under control of the right operator.
- Identify approaches and develop technology for safely and automatically halting commercial and public transit vehicles that violate security guidelines.

RESEARCH, continued

- Conduct research on driver behavior specifically oriented to detecting threatening behavior.
- Participate in mainstream information technology research to assure that transportation industry requirements are included in the development of crisis-oriented electronic and communication systems and to increase the ability to develop large, integrated systems and facilities that are robust and fault-resistant. Work with mainstream information technology and transportation infrastructure interests to establish requirements for hardening sensors, communications, processing centers, and databases against improper access and against misuse, focusing on authentication, verification, and integrity assurance.

PROGRAM

- Work with public safety and security agencies to plan for and include ITS technologies in evacuation and quarantining operations.
- Plan and conduct comprehensive threat and vulnerability assessments of transportation facilities and on the use of vehicles and transportation facilities in mounting attacks.
- Apply surveillance and detection technologies to critical transportation assets.
- Deploy sensors in vehicles and in the infrastructure to identify suspicious vehicles and detect disruptions. Deploy associated network and processing capabilities.
- Deploy technology on a consistent national basis to track and automatically halt commercial and public transit vehicles that violate security guidelines, and to swiftly notify authorities of such violations.
- Upgrade traffic control systems and devices to better handle evacuations and emergency traffic redirection. Conduct periodic full-scale tests of these systems to assure their effectiveness under a range of attack/disaster scenarios.
- Provide better and broader mechanisms for disseminating transportation-related emergency information to the public.
- Conduct a program of outreach to stakeholders both in the transportation sector and elsewhere (e.g., emergency response agencies) to inform them of the security-enhancing resources that ITS can provide. Prepare fact sheets and other documentation to support interactions with non-ITS stakeholders and to provide information on the capabilities ITS provides to assist and support them.

PROGRAM, continued

- Coordinate emergency services with telematics suppliers/in-vehicle systems and other travel information delivery services to facilitate rerouting and evacuation.
- Deploy technology for hardening physical transportation facilities and the information/communications systems that surround them. In particular, harden transportation-related emergency communications facilities and provide backups and alternatives under a range of attack/disaster scenarios. Define cross-agency requirements for communications, resource sharing, and backup.
- Establish mechanisms to archive data on emergency situations and responses for post hoc analysis and future guidance.
- Develop and execute programs to evaluate and improve security measures at major public and privately owned transportation facilities.

"ITS will be a critical tool in securing America's future not only from terrorist attack but also from economic stagnation; it can be a significant agent of institutional change."

Emil Frankel
U.S. DOT Assistant Secretary for Transportation Policy
ITS America's 2002 Annual Meeting and Exposition, April, 2002

Security check at a border crossing.

INSTITUTIONAL

- Determine and establish the institutional structure for deploying surface transportation security on a consistent national basis and smoothly integrating security capabilities into ITS. This necessarily includes funding mechanisms, identification and filling of leadership roles at multiple levels, and clear, comprehensive mechanisms for reporting and feedback.
- Identify common interjurisdictional issues that must be addressed, and provide model legislation and best practices documentation.
- Create the institutional arrangements to coordinate traffic control centers, emergency response centers, operations centers, and traveler information services to better respond to emergencies and keep the public informed.
- Participate, through appropriate study, legislation, and education, in the national effort to ensure the preservation of Constitutional rights while security measures are developed.
- Create and establish the institutional arrangements that underlie the seamless, end-to-end sharing and transmission of freight information, with special attention to freight containers and hazardous cargo.
- Create and establish the institutional arrangements for quick and convenient border crossings by appropriately credentialed people onboard vehicles that cross national borders.
- Create a national ID card for transportation workers that would support rapid and reliable electronic identity and credentials verification. This credential would support rapid shifts of the workforce to respond to a changing threat environment.
- Create programs of community outreach and encouragement to involve local residents in ensuring public transit safety and security.
- Work with the Transportation Security Administration to establish institutional mechanisms for sharing insights and approaches for safety and security across transportation modes (including pipelines), so that developments do not have to be reinvented and lessons do not all have to be separately learned.
- Ensure the existence of public sector mechanisms to accept and integrate safety and security information from private sector sources (e.g., the American Trucking Association's Highway Watch program) to expand the reach of sensors and other information gathering mechanisms.
- Encourage participation in programs like the U.S. State Department's Rewards for Justice Program that provide incentives for reporting on potential security threats. Consider the creation of similar transportation-specific programs.
- Support and participate in ongoing Federal, state, and local programs designed to enhance commercial transportation security, such as Operation Safe Commerce.
- Consult with other countries to learn about their mechanisms for enhancing Homeland Security through ITS.

Stakeholder Roles

State and Local Government and MPOs

- Participate in threat and vulnerability assessment analysis for areas of jurisdiction. Cooperate with adjoining jurisdictions in conducting area-wide assessments and identifying area-wide approaches for enhancing security.
- Deploy and operate systems for threat detection, prevention, and response.
- Establish active inter-agency and inter-jurisdictional cooperation to use ITS for threat detection and emergency response.
- Establish priority scheme for surface transportation system recovery.
- Plan escape routes and evacuation procedures for various scenarios.
- Develop, test, and deploy systems to implement emergency rerouting and evacuation.
- Harden key communications systems from physical threats and hacking; provide redundancy using alternate technologies (e.g., wired and wireless).
- Deploy mechanisms for emergency information dissemination to the public, including direct communications via Highway Advisory Radio (HAR) and Dynamic Message Signs (DMS), information on request via the 511 universal travel information telephone number, plus links to media, telematics providers, etc. Prepare to make use of in-vehicle warning systems as they come on line.
- Revise procurement regulations to facilitate state and local acquisition of ITS technologies.
- Establish a program for training personnel for emergency situations and for exercising emergency plans.

Federal Government

- Fund and guide the development of a comprehensive, multi-modal, national strategy for the surface transportation system that supports Homeland Security and clearly articulates the requirements and needs of state and local agencies, including first responders; the roles, responsibilities and needs of transportation system developers, integrators, owners, operators, and managers in all surface transportation modes (road, transit, rail); and the roles and responsibilities of the private sector.
- Organize and fund research on how to do threat and vulnerability assessment and on the development of appropriate countermeasures in cooperation with such organizations as the American Association of State Highway and

Transportation Officials (AASHTO), the American Public Transportation Association (APTA), the Association of American Railroads (AAR), and the Commercial Vehicle Safety Alliance (CVSA).

- Work in cooperation with such organizations as the American Association of State Highway and Transportation Officials (AASHTO), the American Public Transportation Association (APTA), the Institute for Transportation Engineers (ITE), the American Public Works Association (APWA) and other state and local entities to update state and local DOT emergency operations plans and better define roles and relationships.
- Define programs for sensor deployment, probe data collection, data analysis, threat detection, systematic prevention, and emergency response in cooperation with telematics suppliers, vehicle manufacturers, system integrators, and state and local authorities.
- Fund research and create guidelines for commercial vehicle credentialing and monitoring and for safely automatically halting vehicles that deviate from guidelines.
- Consider rulemaking to mandate the inclusion of monitoring technology in new vehicles and the retrofitting of older vehicles.
- Subsidize cost of additional onboard monitoring equipment (at least for a transition period).
- Fund research and create incentives for the development and deployment of consistent, nationwide in-vehicle warning systems, both to assist rerouting and evacuation in emergencies and to enhance safety for routine travel at work zones, highway rail intersections, and other potentially hazardous locations.
- Support the development of security-oriented ITS standards by ITS-related standards development organizations, both domestically and internationally.
- Evaluate available training packages and consolidate/create a "best of breed" training package for dissemination to local agencies.
- Facilitate and support the conduct of Homeland Security response drills at the local level.
- Promulgate guidelines for emergency information dissemination to the public.
- Encourage and facilitate interagency cooperation at all levels.
- Revise procurement regulations to facilitate Federal acquisition of ITS technologies, for example, technology for container/cargo inspection and tracking at ports and other national border crossings; vehicle/cargo/driver tracking equipment onboard military and other vehicles that serve Federal installations (national parks, military reserves, Pentagon, etc.); ground-based vehicle surveillance technology for sensitive Federal areas; etc.

Public Transportation Agencies

- In cooperation with other public transportation agencies nationwide, FTA, APTA, and the Community Transportation Association of America (CTAA), develop threat and vulnerability assessment processes for transit equipment and facilities.
- In cooperation with other local/regional transportation agencies (all modes), conduct threat and vulnerability assessments.
- In cooperation with FTA, APTA, and CTAA, research, test, evaluate, deploy, and operate systems to deter, detect, react, and recover from threats against the public transportation system. Work with commuter and intercity passenger rail interests to establish travel alternatives and minimize the effect and duration of service disruptions in times of emergency.
- Plan and implement escape and evacuation procedures under various scenarios. Work with other local and regional transportation agencies to develop a coordinated multi-modal plan for transporting responders to emergency sites and transporting the public away from these sites. Participate in area-wide tests of these plans.
- Harden key communications systems from physical threats and hacking; provide redundancy using alternate technologies (e.g., wired and wireless).
- Deploy mechanisms for emergency information dissemination to the public, including direct communications via message signs on transit vehicles and at stops and stations, public address announcements, and links to media.

Emergency Response Services and Emergency Management Services

- Become knowledgeable about the ways in which ITS technologies and the surface transportation network can support all aspects of emergency response including the movement of emergency personnel and the delivery of emergency services.
- Coordinate with appropriate transportation management agencies to develop procedures to exchange information (voice, video and data).
- Coordinate with local government and public transportation agencies to develop plans for better getting responders to emergency sites and for better moving injured and at-risk people to medical care facilities and safe locations through the use of ITS tools and technology.
- Work toward the integration of computer-assisted dispatch systems with local/regional traffic management and operations systems.

Automotive and Electronics Manufacturers

- Conduct research and develop technology for commercial and public transit vehicle monitoring and for their safe automatic halting when they deviate from security guidelines. These mechanisms must exclude the possibility of being tampered with, overridden, or bypassed.
- Lead the development of performance standards and installation guidelines for onboard security equipment.
- Participate in the development of security-oriented communications technology that meets automotive needs.
- Fold installation/integration of ITS safety/security technology into the vehicle manufacturing process. Help establish mechanisms for retrofitting the existing vehicle base.

Telematics Suppliers

- Work with vehicle manufacturers and public officials to develop the onboard technology, communications, and processing services to enable vehicles to be a first line of reporting and surveillance for road and traffic conditions, both for routine operations and in emergency situations.
- Harden key communications systems to guard against their being misused to cause disruptions or hinder responses to emergencies.

Communications Equipment Suppliers and Communications Service Providers

- Help harden key transportation-related communications facilities against natural and human-caused disasters.
- Develop and offer additional safeguards against intrusion, hacking, and fraudulent communications.

The Motor Carrier Industry

- Continue to implement and expand programs that engage commercial vehicle operators in looking out for and reporting suspicious circumstances to public authorities.
- Work with the Federal government to determine the need for and characteristics of a national ID card for transportation workers.
- Participate with other stakeholders in the commercial freight supply chain to work toward a seamless, end-to-end information environment, particularly including the ability to identify and track containers and hazardous cargo.

The Railroads

- Develop and deploy technology to guard against and detect tampering with the track and signal infrastructure and to safeguard major rail transportation centers.
- Participate with other stakeholders in the commercial freight supply chain to work toward a seamless, end-to-end information environment, particularly including the ability to identify and track containers and hazardous cargo.
- Participate with other stakeholders in the personal transportation arena to work toward better coordination of and information about intermodal travel, particularly oriented to providing service alternatives and minimizing the effects and duration of service disruptions in times of emergency.
- Continue the development of the Intelligent Railroad System to enhance the ability to use trains for surveillance and to maximize the effective capacity and flexibility of the rail system.

Ports and Border Crossings

- Ensure the continuous overall operation of these facilities in the event of an attack or other disruption by deploying alternative ITS-based operations plans and communications links between sites remaining functional.

The Transportation Profession

- Make security a priority in the design, development, operation, maintenance, and modernization of the transportation infrastructure.
- Consider the creation of a professional subspecialty in transportation system security.

Academia

- In consultation with the American Association of State Highway and Transportation Officials (AASHTO), the American Public Transportation Association (APTA), and the Institute of Transportation Engineers (ITE), incorporate attention to security and to state of the art of security-related ITS technology into the transportation engineering curriculum.

University and other Research Establishments

- Conduct research, as directed by public and industry priorities, into the development of technologies and processes to detect and ward off threats, to do more effective security-oriented transportation planning, to reduce the extent of damage caused by an attack, and to restore a damaged transportation system to good operating condition as rapidly as possible.
- Facilitate the translation of research results into public policy, professional practice, and industrial action.

ITS America

- Provide leadership on assembling ITS and related stakeholders for information exchange and cooperation in the area of Homeland Security. Provide a forum for airing issues and tradeoffs and for advising government at all levels and private sector transportation stakeholders on ITS-related capabilities and approaches for ensuring security and for supporting a wide range of protection, detection, and response activities both within and outside of the transportation sector.
- Create a partnership with the Office of Homeland Security, U.S. DOT, and other transportation and public safety agencies to develop and implement a national Homeland Security strategy.
- Provide leadership and user input for the development of the Integrated Network of Transportation Information, to support Homeland Security as well as for all the reasons articulated in the *National ITS Program Plan.*
- Serve as a central clearinghouse and a resource for outreach and education on transportation-related security activities. In cooperation with U.S. DOT, actively undertake and support outreach and education to both the transportation community and the general public.
- Work actively with network industries and regulatory agencies to address the threat of cascading failures.
- Help create guidelines for emergency information dissemination to the public.
- Identify and lead the process of addressing legal and institutional issues related to the application of ITS to Homeland Security.
- Identify requirements for and facilitate the development of domestic and international ITS standards and protocols related to Homeland Security.
- Provide leadership on sharing security-oriented ideas and programs with ITS organizations around the world. Provide leadership in facilitating international cooperation in the deployment of ITS in support of security worldwide.
- Support private sector efforts to meet government information security and management reforms.

Standards Development Organizations

- Provide the means for developing domestic and international standards that facilitate Homeland Security, particularly relating to performance requirements for security-oriented technology, including secure and tamper-proof communications. As appropriate, work in cooperation with other SDOs.
- Ensure that standards for communicating among transportation centers and from these centers to traffic control devices, emergency responders, and travelers accommodate requirements for emergency and disaster situations.
- Ensure that standards developed for transportation-oriented security are compatible with other security-oriented standards.

Advocacy Organizations for Drivers and Travelers

- Develop and participate in campaigns of outreach and education to encourage travelers to exercise due caution, but not overreact to potential threats.
- Participate in the process of encouraging community involvement in public transit and roadway security.

inside back cover—blank

Intelligent Transportation Society of America
400 Virginia Ave. S.W., Suite 800
Washington, DC 20024-2730

202.484.4847
www.itsa.org